METHOD AND APPARATUS FOR CRYPTOGRAPHIC KEY ESTABLISHMENT USING AN IDENTITY BASED SYMMETRIC KEYING TECHNIQUE

ABSTRACT

One embodiment of the present invention provides a system for establishing a shared cryptographic key between participating nodes in a network. The system operates by sending a first message from the first node to the second node requesting establishment of a shared key. The second node sends a second message containing identifiers and a message authentication code to a key distribution center (KDC). The authentication code is generated using a second node key belonging to the second node. The KDC recreates the previously created second node key using the second node identifier and a secret key known only to the key distribution center. The KDC then verifies the message authentication code using the second node key. If the message authentication code is verified, the KDC creates a shared key for the nodes to use while communicating with each other. The KDC securely communicates this shared key to the participating nodes